UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/987,912	11/16/2001	Mark Crosbie	10012172	7899

7590 10/05/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
DODDS, HAROLD E	

ART UNIT	PAPER NUMBER
2167	

DATE MAILED: 10/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/987,912	**Applicant(s)** CROSBIE ET AL.	
	Examiner HAROLD E: DODDS	**Art Unit** 2167	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 June 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments with respect to claims 1-21 have been considered but are moot in view of the new ground(s) of rejection.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: ***a device read call*** as in claim 7.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 12, 18 and 19 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

As in claim 12, the claimed *maintaining root and current directions while threads are in the middle of system call processing* was not described in the specification.

As in claim 18, the claimed *selecting step can be based on the outcome of system calls including pass, failure or both* was not described in the specification.

As in claimed 19, the claimed *presenting deposited data to a user space via a device driver in the kernel* was not described in the specification.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 17 and 18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation *the system call path* in the step of triggering data delivery. There is insufficient antecedent basis for this limitation in the claim.

Claim 17 recites the limitation *the tokens.* There is insufficient antecedent basis for this limitation in the claim.

Claim 18 recites the limitation ***the outcome of system calls***. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-21 are rejected under 35 U.S.C. 102(e) as being anticipated by Crosbie et al. [US 2002/0083343 A1].

The applied reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not the invention "by another," or by an appropriate showing under 37 CFR 1.131.

Regarding claim 1, Crosbie teaches ***a method of generating kernel audit data*** comprising:

storing system call parameters or data the parameters point to at the beginning of a system call (paragraph [0205], a user process makes a library call, the call is translated into a system call, if the system call is being audited, header related information: user id, group id, timestamps, process id, etc. as ***system call parameters*** is gathered and stored in temporary buffers); and

triggering data delivery at the end of the system call path (paragraph [0205], once the system call completes as ***the end of the system call path***, the return value and error value are recorded) and

generating an audit record and depositing the audit record in a circular buffer (paragraph [0205], the entire record is placed in a circular buffer in the kernel audit driver).

Regarding claim 2, Crosbie teaches all of the claimed subject matter as discussed above with respect to claim 1, Crosbie further discloses ***each system call that accesses files, storing related file information*** (paragraph [0205]).

Regarding claim 3, Crosbie teaches all of the claimed subject matter as discussed above with respect to claim 2, Crosbie further discloses ***related file information includes file owner or group and the file information is stored before any modifications occur that might affect the file information*** (paragraph [0205]).

Regarding claim 4, Crosbie teaches all of the claimed subject matter as discussed above with respect to claim 1, Crosbie further discloses ***system call parameters that include path name parameters are stored with full path name information*** (paragraphs [0237-0239]).

Regarding claim 5, Crosbie teaches all of the claimed subject matter as discussed above with respect to claim 1, Crosbie further discloses ***the audit record is a tokenized audit record*** (paragraph [0138]).

Regarding claim 6, Crosbie teaches all of the claimed subject matter as discussed above with respect to claim 1, Crosbie further discloses the step of ***reading audit records from the circular buffer*** (paragraph [0205]).

Regarding claim 7, Crosbie teaches all of the claimed subject matter as discussed above with respect to claim 6, Crosbie further discloses ***the reading is triggered using a device read call*** (paragraph [0205]).

Regarding claim 8, Crosbie teaches all of the claimed subject matter as discussed above with respect to claim 1, Crosbie further discloses the step of ***maintaining system wide configuration related data structures*** (FIG. 3) and ***setting selection masks based on such structures*** (paragraph [0761]).

Regarding claim 9, Crosbie teaches all of the claimed subject matter as discussed above with respect to claim 1, Crosbie further discloses the step of ***collecting data in the system call path and formatting the collected data into an audit record*** (paragraph [0105]).

Regarding claim 10, Crosbie teaches all of the claimed subject matter as discussed above with respect to claim 9, Crosbie further discloses ***the collected data is a token stream*** (paragraph [0105]).

Regarding claim 11, Crosbie teaches all of the claimed subject matter as discussed above with respect to claim 1, Crosbie further discloses ***if the circular buffer is full, then either reading some of the audit records from the circular buffer or dropping*** (paragraph [0175]).

Regarding claim 12, Crosbie teaches all of the claimed subject matter as discussed above with respect to claim 4, Crosbie further discloses the step of ***maintaining root and current directions while threads are in the middle of system. call processing*** (paragraph [0239]).

Regarding claim 13, Crosbie teaches all of the claimed subject matter as discussed above with respect to claim 9, Crosbie further discloses the step of ***selecting which data to collect before said collecting step*** (paragraph [0205]).

Regarding claim 14, Crosbie teaches all of the claimed subject matter as discussed above with respect to claim 13, Crosbie further discloses ***selecting step can be based on process, user, group, filename information and/or time intervals*** (paragraph [0205]).

Regarding claim 15, Crosbie teaches all of the claimed subject matter as discussed above with respect to claim 1, Crosbie further discloses the step of ***detecting hard link accesses to a critical file*** (paragraph [0616]).

Regarding claim 16, Crosbie teaches all of the claimed subject matter as discussed above with respect to claim 15, Crosbie further discloses the step of ***maintaining a critical file list for monitoring hard links*** (paragraphs [0451-0461]).

Regarding claim 17, Crosbie teaches all of the claimed subject matter as discussed above with respect to claim 5, Crosbie further discloses ***the tokens are either primitive or composed*** (paragraph [0138]).

Regarding claim 18, Crosbie teaches all of the claimed subject matter as discussed above with respect to claim 13, Crosbie further discloses ***selecting step can be based on the outcome of system calls including pass, failure or both*** [paragraph [0205]).

Regarding claim 19, Crosbie teaches all of the claimed subject matter as discussed above with respect to claim 1, Crosbie further discloses the step of *presenting deposited data to a user space via a device driver in the kernel* (paragraph [0205]).

Regarding claim 20, Crosbie teaches all the claim subject matters as discussed above with respect to claim 13, Crosbie further discloses the step of *configuring which system calls are audited by making ioctl() (control) calls on a device driver* (paragraph [0171]).

Regarding claim 21, Crosbie teaches all the claim subject matters as discussed above with respect to claim 1, Crosbie further discloses the step of *enabling the generation of audit data when a device driver is opened for read, and halting data generation when the device driver is closed* (paragraph [0205]).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HAROLD E DODDS whose telephone number is 571-272-4110. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, JOHN E. BREENE can be reached on 571-272-4107. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Harold E. Dodds

HAROLD E DODDS
Examiner
Art Unit 2167

September 16, 2005

John E Breene

JOHN BREENE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100